SMALL OFFICE REMOTE ACCESS SWITCH QUICK START

Release 7.2

Cabletron Systems

(603) 332-9400 phone
(603) 337-3075 fax
support@ctron.com

Only qualified personnel should perform installation procedures.

NOTICE

You may post this document on a network server for public use as long as no modifications are made to the document.

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

©Copyright 1998 by Cabletron Systems, Inc. All rights reserved.

Cabletron Systems, Inc.
P.O. Box 5005
Rochester, NH 03866-5005

Order Number: 9032449

VIRUS DISCLAIMER

Cabletron Systems has tested its software with current virus checking technologies. However, because no anti-virus system is 100% reliable, we strongly caution you to write protect and then verify that the Licensed Software, prior to installing it, is virus-free with an anti-virus system in which you have confidence.

Cabletron Systems makes no representations or warranties to the effect that the Licensed Software is virus-free.

Copyright © July 1997, by Cabletron Systems, Inc. All rights reserved.

TRADEMARKS

Cabletron Systems, CyberSWITCH, MMAC-Plus, SmartSWITCH, SPECTRUM, and SecureFast Virtual Remote Access Manager are trademarks of Cabletron Systems, Inc.

All other product names mentioned in this manual are trademarks or registered trademarks of their respective companies.

COPYRIGHTS

All of the code for this product is copyrighted by Cabletron Systems, Inc.

© Copyright 1991-1997 Cabletron Systems, Inc. All rights reserved. Printed in the United States of America.

Portions of the code for this product are copyrighted by the following corporations:

Epilogue Technology Corporation
Copyright 1991-1993 by Epilogue Technology Corporation. All rights reserved.

Livingston Enterprises, Inc.
Copyright 1992 Livingston Enterprises, Inc.

Security Dynamics Technologies Inc.
Copyright 1995 by Security Dynamics Technologies Inc. All rights reserved.

Stac Electronics
Stac Electronics 1993, including one or more U.S. Patents No. 4701745, 5016009, 5126739 and 5146221 and other pending patents.

Telenetworks
Copyright 1991, 92, 93 by Telenetworks. All rights reserved.

FCC NOTICE

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment uses, generates, and can radiate radio frequency energy and if not installed in accordance with the operator's manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to correct the interference at his own expense.

WARNING: Changes or modifications made to this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

DOC NOTICE

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

VCCI NOTICE

This is a Class 1 product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は、第一種情報装置（商工業地域において使用されるべき情報装置）で商工業地域での電波障害防止を目的とした情報処理装置等電波障害自主規制協議会（VCCI）基準に適合しております。
従って、住宅地域またはその隣接した地域で使用すると、ラジオ、テレビジョン受信機等に受信障害を与えることがあります。
取扱説明書に従って正しい取り扱いをして下さい。

CABLETRON SYSTEMS, INC. PROGRAM LICENSE AGREEMENT

IMPORTANT: Before utilizing this product, carefully read this License Agreement.

This document is an agreement between you, the end user, and Cabletron Systems, Inc. ("Cabletron") that sets forth your rights and obligations with respect to the Cabletron software program (the "Program") contained in this package. The Program may be contained in firmware, chips or other media. BY UTILIZING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNUSED PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

CONTENTS

Using Quick Start 7

Cabling 8

The PC to CyberSWITCH Connection 8
Using a10BaseT Hub LAN Connection 9
Using a10BaseT Direct LAN Connection 10
Using a 10Base2 (BNC) LAN Connection 12
Using an AMP Connection 13
For Out-of-Band Management 13
For LAN Replacement 13
For Local Console Access 13
Using an AMP Connection for LAN Replacement or Local Console Access 14
The ISDN Connection 15
CyberSWITCHs with Internal NT-1s 15
CyberSWITCHs without Internal NT-1s 16
CyberSWITCHs Requiring DSUs 17
Connection Instructions 17
Termination Switches 17
The POTS Connection 18
The Power Connection 19

Basics 20

Reading the LED Indicators 20
Accessing the Release Notes 20
Safety Considerations 21
Accessing the CyberSWITCH 21
Connecting an Administration Console 21
Changing the Baud Rate 22
Telnet Connection 22
AMP Connection 23
Login on the CyberSWITCH 23
Making Configuration Changes 23
Upgrading Software 24
Local Software Upgrade 25
Local Upgrade of the Second Stage Boot (SSB) 26
Local Upgrade of the Operational Software (OSW) 26
Remote Software Upgrade 27
Remote Upgrade of the Second Stage Boot (SSB) 27
Remote Upgrade of the Operational Software (OSW) 28
Change Defaults to Secure System 29
Return Configuration to Factory Defaults 30
Initial Installation Steps 30
Beginning the Configuration Process 30
Physical Resource Configuration 31

Connectivity 32
Overview 32
Connecting One Cabletron Product to another via PPP 32
Bridge to Bridge Configuration 32
Configuration for Site "Central" 32
Configuration for Site "Remote" 33
IP Router to IP Router Configuration 34
Configuration for Site "Central" 34
Configuration for Site "Remote" 35
IPX Router to IPX Router Configuration 36
Configuration for Site "Central" 36
Configuration for Site "Remote" 37
AppleTalk Router to AppleTalk Router Configuration 38
Configuration for Site "Central" 38
Configuration for Site "Remote" 39
Special Features 41
Configuring the POTS Option 41
Configuring the Encoding Standard 41
Configuring POTS Line Information 42
Configuring POTS Information Per Device 42
Configuring Hardware Filters 43
Troubleshooting 45
Local Area Network LED Indicators 45
Wide Area Network LED Indicators 45
Service Indicator 46
Service Indicator Remains Lit 46
Service Indicator Blinks 47
Index 48

USING QUICK START

This guide is for the CSX154 and the CSX155; collectively known as the CSX150 Series. To simplify the documentation, throughout this guide we will refer to these products as CSX150.

Follow the instructions in this guide for installing the CyberSWITCH, powering it up, and making any necessary changes to the default configuration values. Perform the steps in order; skipping the sections that pertain to options you will not use.

We include the following chapters:

- *Cabling*
  Provides you with instructions for connecting the CyberSWITCH to your PC, several methods for ISDN connections, and completing a POTS connection.

- *Basics*
  This chapter gives detailed instructions on the initial installation steps that are required for all CyberSWITCH configurations.

- *Connectivity*
  This chapter gives instructions for connecting two of our products together via PPP. Separate instructions are provided for bridging, IP, IPX, and AppleTalk configurations.

- *Special Features*
  The Special Features sections discusses two features, POTS and Hardware Filtering, that are unique to the CSX150.

- *Troubleshooting*
  Provides an explanation of the CSX150 LED indicators: how to interpret them and corrective actions to take.

CABLING

CyberSWITCH cabling includes the following:

- connecting your PC to the CyberSWITCH
- providing an ISDN connection for the CyberSWITCH
- optional: connecting telephone devices to the CyberSWITCH using a POTS connection
- connecting the CyberSWITCH to the provided power supply

This chapter describes each of the cabling processes.

Note: If a cable you need is not among the cables included with your CyberSWITCH shipment, order the cable separately through Cabletron or your distributor.

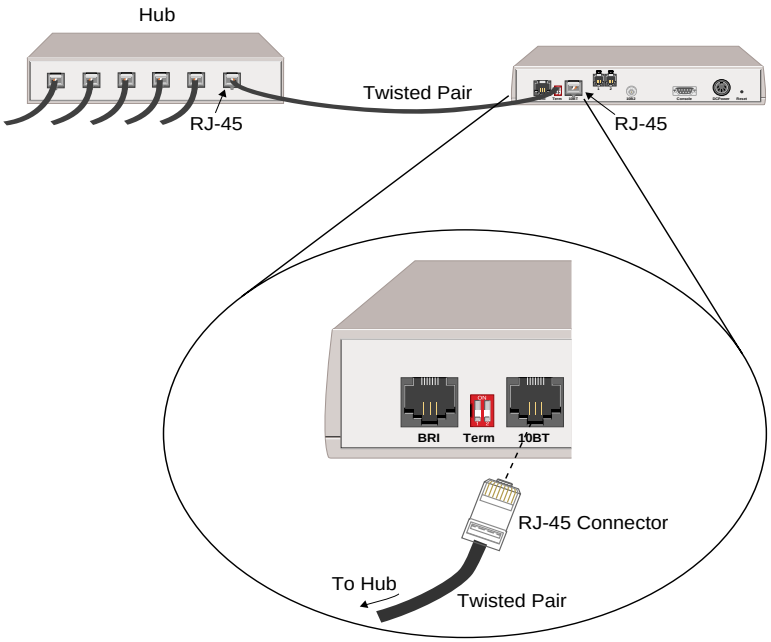
THE PC TO CYBERSWITCH CONNECTION

There are several options available for connecting your PC to the CyberSWITCH. There are three LAN connection methods (using a 10BaseT Hub, 10BaseT Direct, or 10Base2 connection), or you can use an AMP connection. Refer to the section that describes the PC to CyberSWITCH connection you will use.

USING A10BASET HUB LAN CONNECTION

If you plan on using a 10BaseT Hub to connect one or more PCs to the CyberSWITCH, this is the type of connection you will use.

Use the following graphic and instructions to complete the connection.



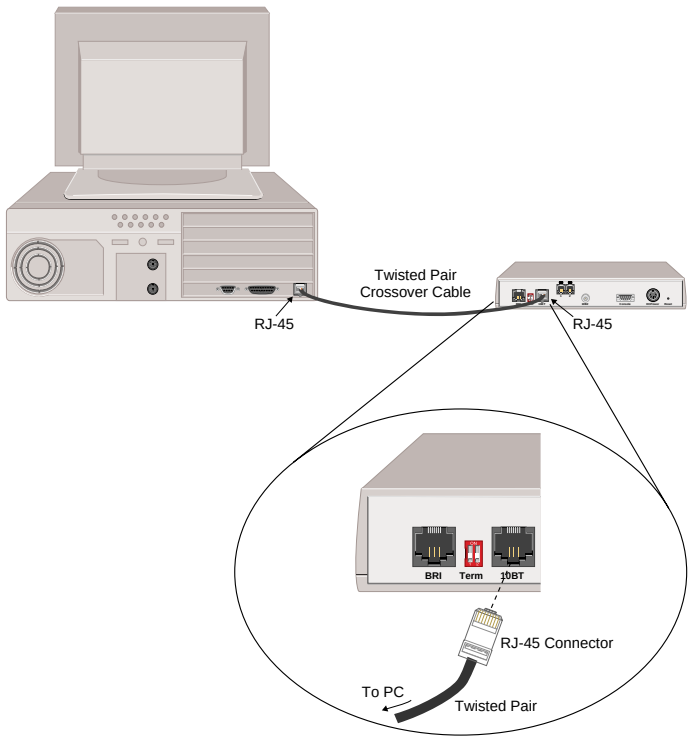
1. Connect your PC to the Hub using the supplied straight through cable (RJ-45 connectors with twisted pair).

2. Connect the Hub to the CyberSWITCH, also using straight through cable.

USING A10BASET DIRECT LAN CONNECTION

If you plan on connecting your PC directly to an CyberSWITCH, this is the type of connection you will use.

Use the following graphic and instructions to complete the connection.

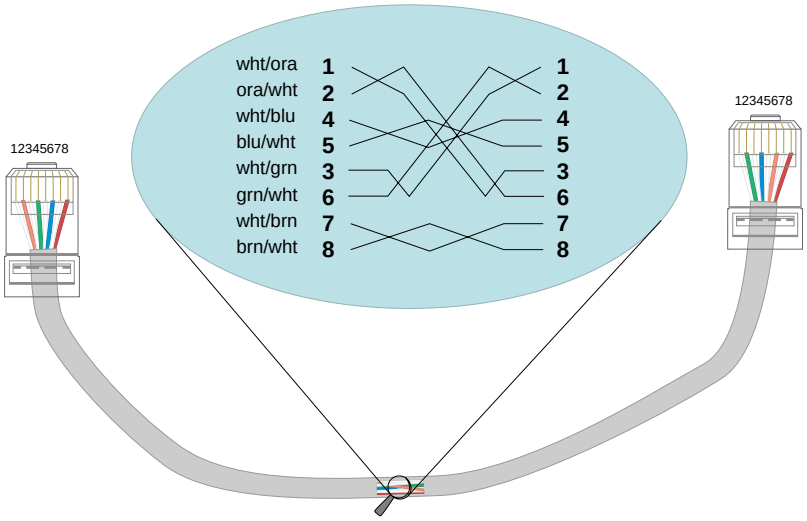


1. Connect your PC to the CyberSWITCH using a crossover cable. This cable is a custom made cable using RJ-45 connectors and twisted pair. Order this cable through Cabletron or your Distributor.

   The crossover cable allows your PC and the CyberSWITCH to communicate directly, without a Hub between them.

If you wish to make your own, the pinouts for the crossover cable's connectors are color-coded as follows:

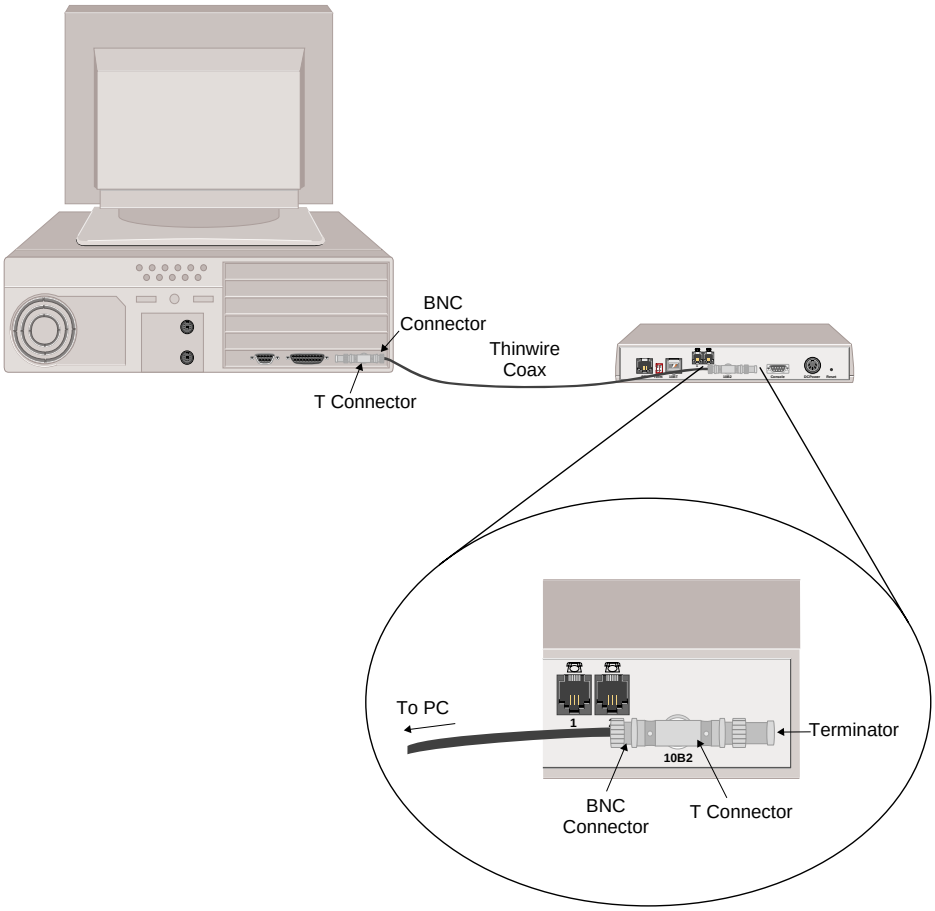
Ethernet 10Base-T Crossover Patch Cord



USING A 10BASE2 (BNC) LAN CONNECTION

If you plan on connecting your PC to an CyberSWITCH using the 10Base2 LAN port, this is the type of connection you will use. Note that the 10Base2 LAN port is an optional CyberSWITCH feature.

Use the following graphic and instructions to complete the connection.



1. Attach one BNC T-connector to the 10Base2 port of your PC and one to the10Base2 port of the CyberSWITCH.

2. Connect one end of a 10Base2 cable (BNC connectors with thin wire coax) to your PC's BNC T-connector, and the other end to the CyberSWITCH's BNC T-connector.

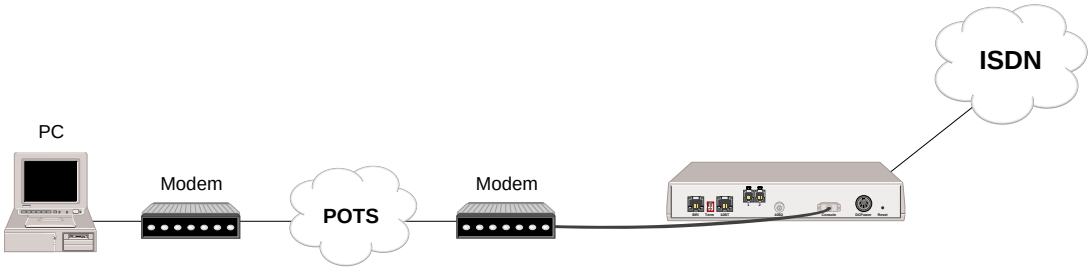
3. For each BNC T-connector, the other side of the T-connector must either have another 10Base2 cable connection, or have a BNC terminator as shown in the above graphic.

USING AN AMP CONNECTION

If you want to use out-of-band management, want a replacement for a LAN connection, or want local console access, you need an asynchronous management port (AMP) connection.

FOR OUT-OF-BAND MANAGEMENT

Out-of-band management allows you to manage the CyberSWITCH from some remote location without making use of the LAN or WAN connections. Out-of-band refers to the fact that you are not using normal data channels. The following graphic illustrates an out-of-band connection.



Connection instructions:

1. At the CyberSWITCH:
   - complete your LAN and WAN (ISDN) connections
   - using the *ampconf* Manage Mode command, configure the CyberSWITCH for the modem you will use
   - connect a modem to the CyberSWITCH (using the *Console* connection)
   - connect the modem to the analog line (use a standard PC modem RS232 cable for this, do not use the supplied cable)

2. At the remote management site:
   - connect the managing PC to a modem
   - connect the modem to the analog line (use a standard PC modem RS232 cable for this, do not use the supplied cable)

FOR LAN REPLACEMENT

There are two reasons for wanting a LAN replacement:

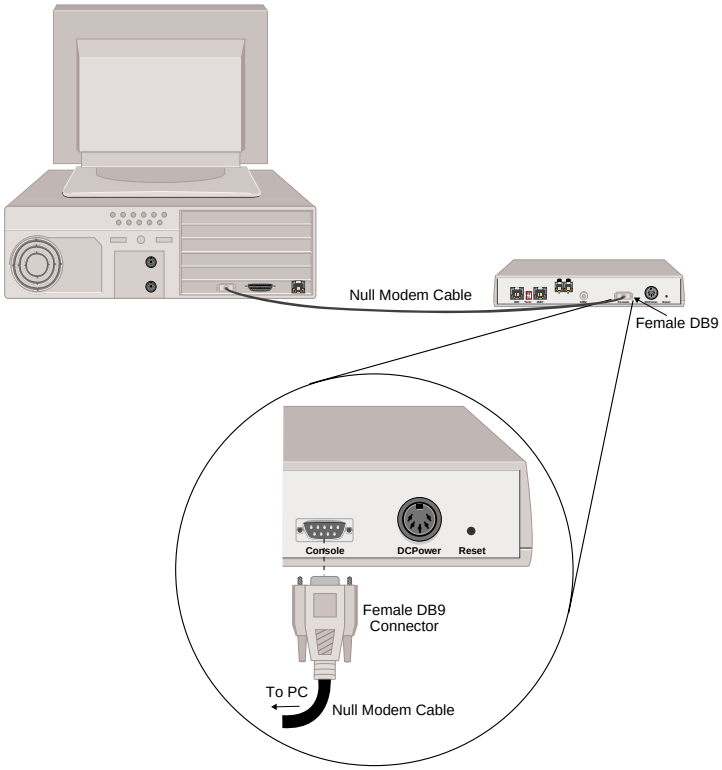
- to provide a connection to manage the CyberSWITCH without using a LAN connection, or
- no LAN connection is possible because your PC does not have a NIC card.

FOR LOCAL CONSOLE ACCESS

You may use the AMP connection for local console access. With this type of access allows you to use a directly connected PC, monitor, and keyboard to manage your CyberSWITCH.

USING AN AMP CONNECTION FOR LAN REPLACEMENT OR LOCAL CONSOLE ACCESS

Regardless of why you want to use an AMP connection, the cabling is the same. Use the supplied cable. To complete the cabling, refer to the following graphic and instructions.



1. Connect one end of a Null Modem to your PC serial port.

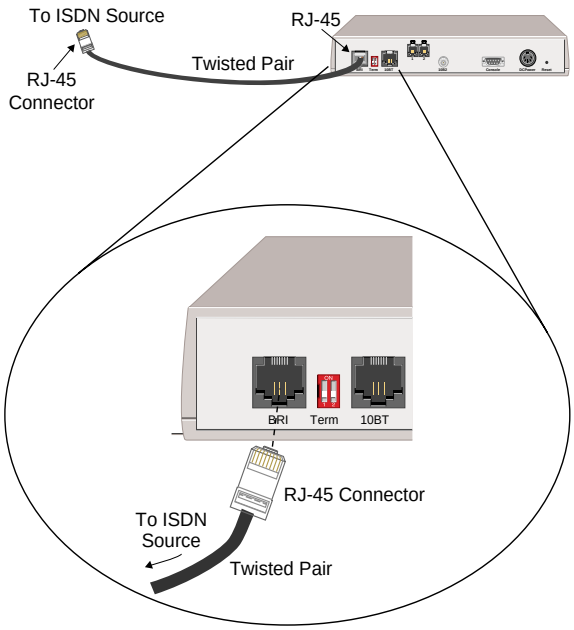
2. Connect the other end of the Null Modem to the CyberSWITCH's serial port labeled *Console*.

THE ISDN CONNECTION

No matter which LAN connection method you use, you must have an ISDN connection. This connection is your link to the outside world through ISDN lines. There is more than one ISDN connection method possible. The method you use depends on the country you live in, and whether or not you have an CyberSWITCH with the internal NT-1 option.

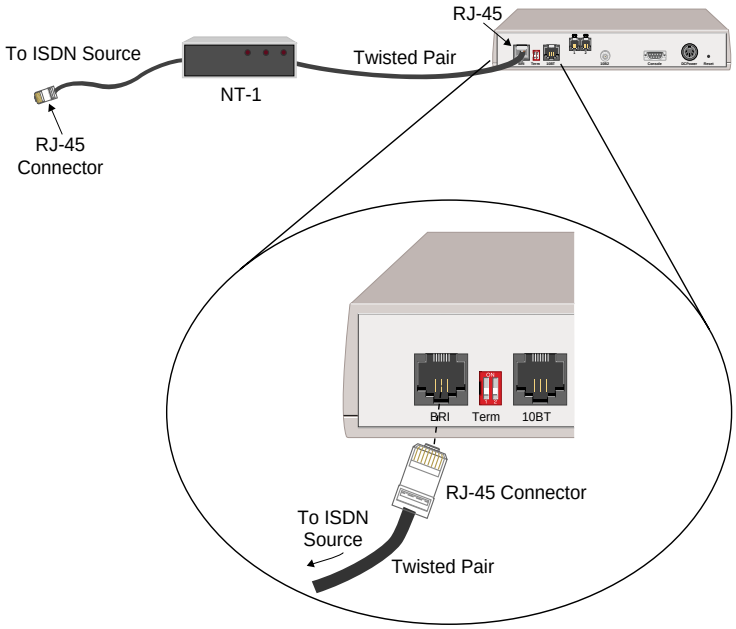
CYBERSWITCHS WITH INTERNAL NT-1S

For countries that require the customer to supply the NT-1s (for example, the United States), an CyberSWITCH is available with an internal NT-1 option.



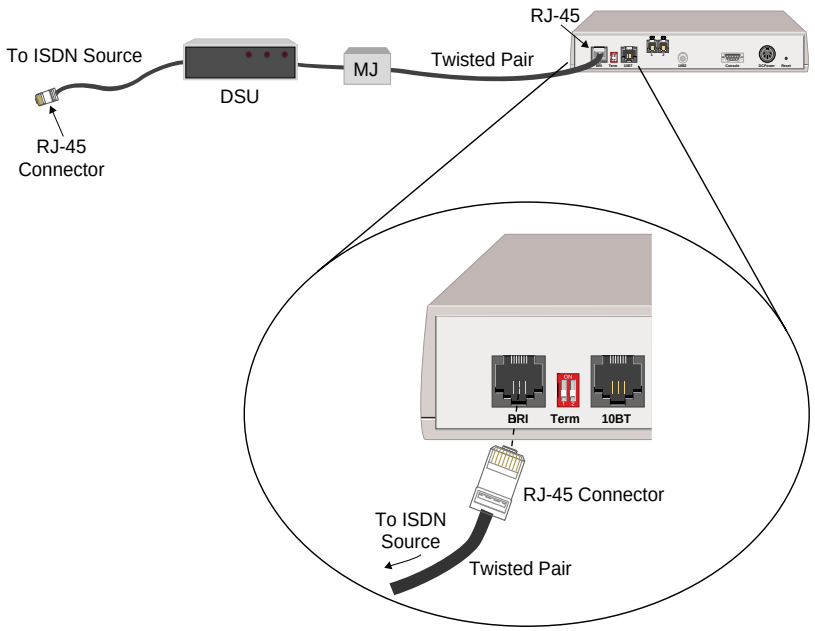
CYBERSWITCHS WITHOUT INTERNAL NT-1S

If you require an NT-1 and you purchase an CyberSWITCH without an internal NT-1, you will need to use an external NT-1 in your connection to the network. Issuing the *ver* command will tell you whether or not your CyberSWITCH has an internal NT-1.



CYBERSWITCHS REQUIRING DSUS

For countries that require DSUs (for example, Japan), your CyberSWITCH will not have an internal NT-1. You will need to use an external MJ and DSU in your connection to the network.



CONNECTION INSTRUCTIONS

1. If you *are not* using an CyberSWITCH with an internal NT-1:
   a. Connect the CyberSWITCH to required intermediary devices (NT-1, or a MJ and CSU) using a straight through cable (RJ45 connectors and twisted pair).
   b. Connect the intermediary device to the network (for example, to your ISDN phone jack).

2. If you *are* using an CyberSWITCH with an internal NT-1, simply connect the CyberSWITCH to the network using a straight through cable (RJ45 connectors with twisted pair).

TERMINATION SWITCHES

On the CyberSWITCH's back panel (to the right of the BRI connector) there are a pair of termination switches for multipoint connections. These switches are labeled *Term*. These DIP switches control the terminating resistors for the Basic Rate Interface.

You must set both switches in the same direction or improper operation may result. The small arrow points in the direction of the *on* position. When the switches are *on*, the resistors for the connector are providing termination for the BRI line. Conversely, when the switches are *off*, the resistors for the connector are *not* providing termination for the BRI line.

On an S/T interface, it is important to have the switches set correctly. On a U interface, the circuitry is intended to operate properly no matter which switch setting is used; however, optimum operation is achieved with the switches *off*.

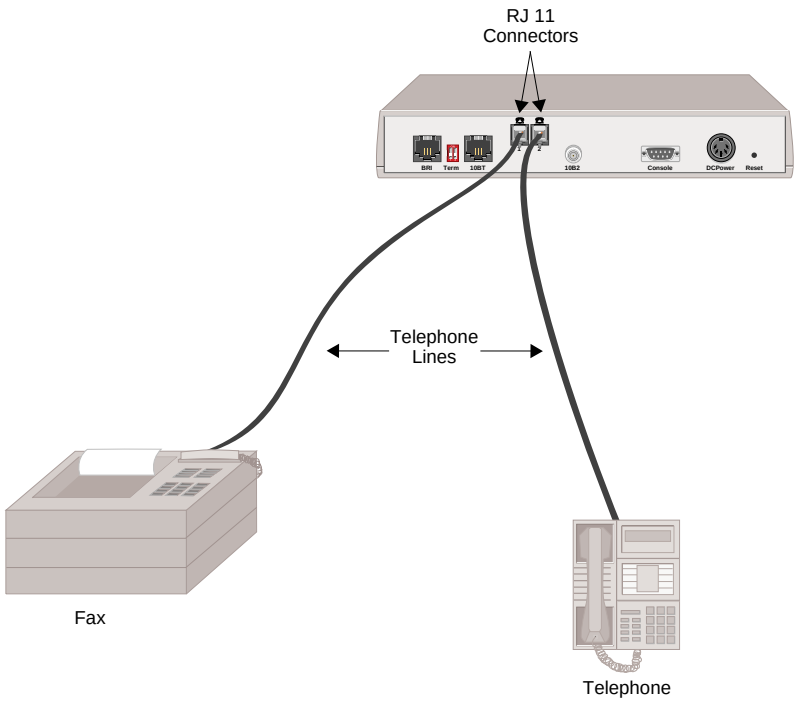
THE POTS CONNECTION

The dual-line, Plain Old Telephone Service (POTS) feature allows one or both of the ISDN B-channels to alternatively be used with traditional phone equipment (for example, a phone, a fax, or an answering machine). When used with a LAN or AMP connection, this allows you to use one ISDN line for both data and voice.

Note: The CyberSWITCH must have a power source for operation. Since POTS is an integral feature of the CyberSWITCH, it too needs power. When power is off, you loose your CyberSWITCH phone service. Therefore, do not rely on the phones connected to the CyberSWITCH ports for emergency service (i.e., 911). In a home office or small office situation, we recommend retaining a standard analog phone line for emergencies.

The POTS interface acts as a simple PBX or Key System. Note that the POTS interface responds to DTMF (Dual Tone Multifrequency) signaling only; it does not support pulse dialing.

Use the following graphic and instructions to complete the connection.



1. Insert one end of a telephone line into Jack 1 (see above graphic).

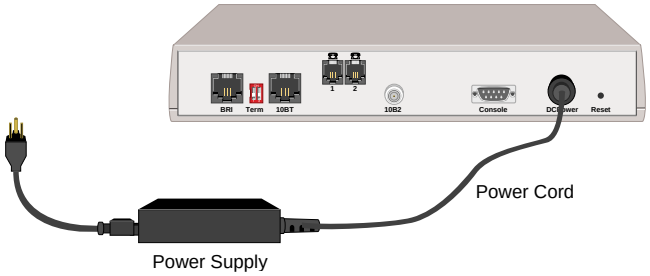
2. Insert the other end of the line into your telephone equipment.

3. If you are connecting a second piece of telephone equipment, repeat the above steps using Jack 2.

THE POWER CONNECTION

Note: Before you plug in the CyberSWITCH, consider the following:

- make sure the CyberSWITCH is well ventilated
- insert the power cord into the wall last, after you attach the power supply and power cord to the CyberSWITCH.



Connection instructions:

1. As shown above, insert the power supply into outlet labeled *DC Power* on the back of the CyberSWITCH.

2. Insert the female adapter of the power cord into the other end of the power supply. The power cord included with your CyberSWITCH is country specific.

3. Insert male end of power cord into electrical outlet.

BASICS

Once your cabling is complete, power on the CyberSWITCH simply by plugging its power cord into an electrical outlet. During the powering on sequence, the CyberSWITCH's LED indicators provide valuable information. We provide you with instructions for "reading" the LED indicators.

After powering on, but before putting the CyberSWITCH into normal operation, we recommend that you read the Release Notes for important information.

READING THE LED INDICATORS

Refer to the following graphic for locating specific LED indicators:

During the CyberSWITCH's power on sequence, you should see the following:

1. After plugging the CyberSWITCH in, the power indicator will light up and stay lit.

2. The service indicator will light up for the duration of the initialization tests. It will then blink if there is a problem. For example, it will blink if your LAN is not properly terminated. For further information, refer to *Trouble Shooting*.

3. The RX indicator blinks during port testing.

4. If you are using a 10BaseT connection, the 10BaseT indicator will light up if the connection is good.

5. The SYNC indicator will light up if layer 1 comes up.

6. The D-CHAN indicator will light up if the data link comes up.

7. After power on is complete, check the log messages (issue the `dr` console command) for any warning or error messages.

ACCESSING THE RELEASE NOTES

The *Release Notes* provide release highlights and important information related to this release that should be reviewed before you begin the system's installation and configuration.

The Release Notes are located on the *CD*

Insert the CD into the drive, change to the proper directory, and enter the following command at the DOS prompt:

[CD-ROM drive]:\[platform directory][ISDN standard directory][option directory]> type REL_NOTE.TXT | more

For example, if your CD-ROM is designated as drive D, you are installing is CSX150, using US ISDN standards and the IP/IPX option, you would use the following path:

D:\CSX150\US\IPX> type REL_NOTE.TXT | more

SAFETY CONSIDERATIONS

The CyberSWITCH contains a lithium battery to support its time-keeping functions. It is a long-lasting battery, and was not intended to be user-replaceable. In the unlikely event that you have a problem with the battery, contact your distributor for replacement.

CAUTION: Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.

ACCESSING THE CYBERSWITCH

There are three ways to access the system. The first method uses a console connection through the console port on the back of the system, and connects up either a terminal or a workstation/PC executing a terminal emulation program. The second method is to Telnet to the system. The third method uses an AMP connection. We describe each of these methods below.

CONNECTING AN ADMINISTRATION CONSOLE

There are two ways to set up a console connection. The first way is to simply connect up an ASCII terminal to the console port on the back of the system. This method can only be used to configure or manage the system. To install or upgrade system software, you must use the second method described below.

The second way is to use a PC or workstation to connect to the system. The CyberSWITCH does not have a CD-ROM drive. Therefore, you must upgrade or install the software through an attached PC, UNIX workstation, or any device that meets the following requirements:

- has a CD-ROM drive
- provides an RS232 terminal program
- has X-Modem communications capability (required for software upgrade only)
- has ASCII transfer capability (required for SSB recovery)

Any computer or terminal that meets these requirements and connects to the administration port on the system can operate as an administration console.

Connect one end of a null modem cable to the console port on the CyberSWITCH, and the other end to the communication port on the PC. On the PC you must then execute a communication package to emulate a terminal (VT100). Your communication package should support file transfer (Xmodem and ASCII) for software upgrades and installations.

Use the following default values for your communication package:

Baud rate	9600
Parity	None
Data bits	8
Stop bits	1
Duplex	Full

CHANGING THE BAUD RATE

The baud rate is changeable. The default rate performs well for configuration changes. A faster rate is useful, however, to download new software upgrades to your system.

To change the baud rate through CFGEDIT:

1. Select *Physical Resources* from the main menu.
2. Select *Data Line* from the physical resources menu.
3. Follow the instructions to make changes to the ASYNCMDM.
4. When asked, enter the baud rate you want to use.
5. Step through the remaining parameters. The last entry will ask you if you would like to save your changes. Answer *yes*.
6. To make the new baud rate effective, restart the system (with the `restart` command).
7. Change the communications package you are using to the same baud rate.

To change the baud rate using Manage Mode:

1. Enter the Manage Mode by entering the following command:
   `>manage`
2. At the Manage Mode prompt, enter the following command:
   `>ampconf change`
3. Follow the on-screen instructions for changing the baud rate.

TELNET CONNECTION

You can access the CyberSWITCH with Telnet. To do this, you must use Telnet client software.The CyberSWITCH has default IP addresses configured to allow Telnet access. The default LAN IP address is 1.1.1.1. To access the CyberSWITCH you must set the device's IP address to be on the same subnet as the CyberSWITCH. We recommend that you use 1.1.1.2 and do this on a LAN that is not connected to the internet. Then place the CyberSWITCH on the LAN and Telnet to the address.

This default address allows immediate access to the system for installation purposes. Be sure to change this IP address as soon as possible to one on your local subnet.

Note: Do NOT place more than one CyberSWITCH on a LAN with the default setting. With both having the same IP address, unpredictable results will occur.

You may also Telnet in via the WAN connection, however, how to set it up with the default configuration will not be described in detail in this guide. The general procedures are:

1. Connect the system to the ISDN line.

2. From a remote device that supports UnNumbered IP connections, dial in as a PPP CHAP device USER1 (USER1 as secret). The address on the CyberSWITCH to Telnet to is 1.1.1.1.

3. From a remote device only supporting numbered IP connections, set up an IP Address 2.2.2.3 and have it dial as a PPP CHAP device USER2 (USER2 as secret). The address on the CyberSWITCH to Telnet to is 2.2.2.2.

After you make a Telnet connection, enter your login id and password. Then you will be presented with a system prompt and you can enter commands at that time.

AMP CONNECTION

You may use the AMP connection for local console access. With this type of access, use a directly connected PC, monitor, and keyboard to manage your CyberSWITCH. Refer to *Cabling* for AMP cabling instructions.

LOGIN ON THE CYBERSWITCH

Once you have a connection to the CyberSWITCH, you will be presented with a prompt to enter your log in id. Use *admin* as the login id. You will then be prompted for a new password, so choose a password that you will remember. If your software was previously accessed by your distributor, your password will be *admin* (in lower case).

After you have logged in, you many enter any command at the system prompt.

MAKING CONFIGURATION CHANGES

We provide three configuration tools to set up and / or alter your configuration. These tools are:
- Set-Up Utility, the basic configuration utility, for basic configurations
- CFGEDIT, the full configuration utility
- Manage Mode, the dynamic management utility

Using Set-Up Utility is a fast and easy way to configure your system. However, it was designed to handle basic configurations, not for more complex configurations. If you have a more complex configuration, you may find it convenient to begin your configuration using our Set-Up Utility, get the system up-and-running, then use the more robust CFGEDIT utility to fine tune your configuration. The Set-Up Utility is located on the CD included with your CyberSWITCH. Instructions for installing and running the Set-Up Utility are in the pamphlet accompanying the CD.

For a more complex configuration, CFGEDIT is the comprehensive utility you may wish use to initially set up your system; you may use it later to make configuration changes as well. However, CFGEDIT is NOT dynamic. This means you will have to interrupt normal system operations in order to update configuration files. To begin the configuration process:

Start up the configuration editor, CFGEDIT. Your machine should be at the system prompt. To start up the configuration editor simply type:

```
[system name]> cfgedit
```

The main configuration menu should now be displayed. Refer to *Connectivity* for the configuration steps required for the device you wish to connect.

Note: If you are prompted for configuration information that you don't know, use the default. This document will provide detailed instructions if something other than the default is required.

Manage Mode provides a real-time management mechanism that allows you to change the configuration, without interrupting the current execution state of the system software. But, because it is dynamic, Manage Mode does have its limitations. So, when making configuration changes, you usually need to use a combination of both of these two tools. Enter the Mode by entering the >*manage* command at the system prompt. To save your changes, enter the *commit* command. To leave the Manage Mode, enter the *exit* command.

UPGRADING SOFTWARE

An upgrade of system software may involve the upgrade of two components: the second stage boot (SSB) and the operational software (OSW). For most upgrades, if you have a working SSB, you will only need to upgrade the OSW. If the new OSW requires an upgraded SSB, you will be alerted in the Release Notes.

The CyberSWITCH offers two different methods of upgrade—local and remote.

- To perform a local upgrade refer to the section titled *Local Software Upgrade*. (A local upgrade is performed via the administration console attached to the system's RS232 port).
- To perform a remote upgrade refer to the section titled *Remote Software Upgrade*. (A remote upgrade is performed over the network using Telnet and TFTP).

The *CSX150 CD* contains installation, user documentation and upgrade files. The file structure is as follows:

Directory	*Contents*
<*ROOT*>\	installation program files (SETUP.*)
CSXDOCS\	CSX150 user documentation and Acrobat reader
\CSX156\JAPAN\ipipx	UPGRADE.OSW, DEFLTCFG.OSW, RECOVER1, RECOVER2, REL_NOTE.TXT
\CSX156\JAPAN\ipipx.fr	UPGRADE.OSW, DEFLTCFG.OSW, RECOVER1, RECOVER2, REL_NOTE.TXT
\CSX156\JAPAN\ipipx.x25	UPGRADE.OSW, DEFLTCFG.OSW, RECOVER1, RECOVER2, REL_NOTE.TXT
\CSX156\JAPAN\ipipxat	UPGRADE.OSW, DEFLTCFG.OSW, RECOVER1, RECOVER2, REL_NOTE.TXT
\CSX156\JAPAN\ipipxat.fr	UPGRADE.OSW, DEFLTCFG.OSW, RECOVER1, RECOVER2, REL_NOTE.TXT
\CSX156\JAPAN\ipipxat.pkt	UPGRADE.OSW, DEFLTCFG.OSW, RECOVER1, RECOVER2, REL_NOTE.TXT
\CSX156\JAPAN\ipipx.pkt	UPGRADE.OSW, DEFLTCFG.OSW, RECOVER1, RECOVER2, REL_NOTE.TXT
\CSX156\JAPAN\ipipxat.x25	UPGRADE.OSW, DEFLTCFG.OSW, RECOVER1, RECOVER2, REL_NOTE.TXT

For system upgrade, you will need to follow one of the above-mentioned upgrade paths (*\product name\country\protocol or access package)*. This path not only depends upon product, but also the ISDN Standard you will be using and the software options you have purchased. For example:

- If you are installing a CSX156 in a geographical area that uses JAPAN ISDN standards, and you have purchased the IP / IPX software option, use the files found in the *\CSX156\JAPAN\ipipx* directory.
- If you are installing a CSX156 in a geographical area that uses JAPAN ISDN standards, and you have purchased the IP / IPX / AppleTalk / Frame Relay software options, use the files in the *\CSX156\JAPAN\ipipxat.fr* directory.

LOCAL SOFTWARE UPGRADE

To perform a local upgrade, use any valid local administration console as defined in *Connecting an Administration Console*. Update the SSB first, if the Release Notes indicate this is necessary, and then follow with the update of the OSW.

LOCAL UPGRADE OF THE SECOND STAGE BOOT (SSB)

To locally upgrade the second stage boot (SSB), follow these steps:

1. Restart the CyberSWITCH.

2. When "Waiting for Commands:" appears on the system screen, enter the following command:
   recover

3. Wait for the system to respond with the prompt "Ready for Hex Download". Using your communications program:
   - Select ASCII to be the protocol used for the file transfer.
   - Change character spacing to "0". (This may be called by another name in some communications packages. For example, some programs call it character pacing.)
   - Set line spacing (or pacing) to "0".
   - insert the CSX CD into the CD drive of your administration console.
   - Enter the name of the file to be transferred, using the complete pathname. For example, `D:\CSX150\US\IPIPX\RECOVER1.`

4. You will receive a message if the upgrade completes successfully. The system will then automatically reboot.

LOCAL UPGRADE OF THE OPERATIONAL SOFTWARE (OSW)

To locally upgrade the operational software (OSW) of your system, follow these steps:

1. Change the CyberSWITCH system's baud rate to be the fastest baud rate supported by your communications package (up to 115.2 Kbps). Change the baud rate as described on page 22.

2. Login to the CyberSWITCH as admin.

3. At the system prompt, enter the command:
   flash update
   This message is displayed:

4. At this time you should press "Y" <RET>. After 30 seconds, you will see the startup messages.

5. When it displays the download message, "Ready for Xmodem Download," return to your communication program and use the "XMODEM" protocol for the software download.

6. Enter the name of the file that is to be downloaded, using the complete pathname. For example, `D:\CSX150\US\IPIPX\UPGRADE.OSW`.

   Note: Your terminal program may display a character for the NAK control code, typically the character "§". This will be displayed every second until the download has started.

7. After the file has been downloaded, the system will reboot automatically and load using the new software.

REMOTE SOFTWARE UPGRADE

Note: For security purposes, we recommend that you disable the TFTP Server after the upgrade is complete.

To remotely upgrade the system, you are required to have a PC / workstation that is connected to the system's network. It must have the following features:

- ability to read CDs
- TELNET client
- TFTP client

To perform a remote upgrade, first upgrade to the latest SSB, if required, then upgrade the OSW. The Release Notes will indicate whether or not the SSB needs to be upgraded.

Note: If, during a remote upgrade, the compressed file set cannot be uncompressed into the Flash File System due to a lack of space, the compressed file set will not be deleted from the Flash File System and the previous version of the OSW will be booted. If the OSW determines there is a compressed file set (a file suffix of .OSW) in the Flash File System, then the following message is logged in the system log:

```
OSW, <OSWFileName>, found in the Flash File System. The OSW has not been
    updated from this file due to insufficient Flash File System space.
    Please delete unnecessary files from the system.
```

It is possible that you will not have enough room in the `\SYSTEM` directory to TFTP the upgrade file to the system. In this case:

- Delete all files in the directory except `nex.bin` and `iop.bin`.
- Issue a *`flash reclaim`* command to gain the lost space (this will destroy the backup copy of your configuration, you will be unable to issue restore command unless you have saved at least one set of changes).
- If the upgrade still fails, delete the `nex.bin` and `iop.bin` and again reclaim the space. Your upgrade should now work. IMPORTANT: *Do not* restart the CyberSWITCH until the upgrade is complete.

If you are upgrading from a previous version of system software, the above message will not be displayed. In this case, the system continually restarts, attempting to install the OSW package each time.

REMOTE UPGRADE OF THE SECOND STAGE BOOT (SSB)

WARNING:
If power is lost on the remote CyberSWITCH during this process, a local upgrade of the SSB may be necessary before the system can again function.

To remotely upgrade the SSB, follow these steps:

1. Telnet to the CyberSWITCH and login as admin.

2. Enable TFTP, the TFTP client, and the TFTP server with admin access rights (see page 28.)

3. Using the TFTP client on the remote workstation, TFTP the `recover1` file to the CyberSWITCH in binary mode. Be sure to use the file's full pathname. The exact method to transfer varies, depending upon your TFTP client.

4. At the system prompt, recover the SSB by issuing the following command:
   ```
   flash recover
   ```
   The system will ask you if you are sure you want to remotely recover the SSB, and warn you of the potential risk in case of a power failure while the SSB is being recovered. Answer "yes" to the prompt. The window of vulnerability ends after 5 or 10 seconds, when the system tells you that the SSB was successfully recovered.

5. After the recovery, delete the file by issuing the command:
   ```
   del \system\recover1
   ```

6. Recover lost space with the command:
   ```
   flash reclaim
   ```

Console Messages during SSB Upgrade:

Message	*Suggested Action*
can't open recover file	If you entered a filename after the flash recover command, makes sure that the file exists on the system. If you did not enter a filename, make sure that \SYSTEM\RECOVER 1 exists on the system.
not enough DRAM to create binary image	Remove DRAM-greedy activities on the system, such as connections to other devices, compression, and authentication. Reboot if necessary.
error in recovery file	Make sure that the recover file that you are using is the same as the one on the CSX CD. Delete, Recover, and reTFTP if necessary.
Unable to remotely recover SSB	Hardware failure in the boot device. Contact your distributor immediately for a replacement.
successfully updated	The SSB has been successfully updated.

REMOTE UPGRADE OF THE OPERATIONAL SOFTWARE (OSW)

To remotely upgrade the operational software, follow these steps:

1. From the PC / workstation, Telnet to the CyberSWITCH and login as admin.

2. Verify that the system is ready to receive TFTP upgrades:
   - Enter MANAGE MODE by typing *`manage`* <RET> at the system prompt.
   - Using the MANAGE MODE command *`tftp`*, verify that:
     - TFTP feature is enabled
     - TFTP server is enabled
     - TFTP server is assigned ADMIN file access rights

- Using the MANAGE MODE command ***fileattr***, verify that:
  - ADMIN has READ/WRITE access to CONFIG files
  - ADMIN has READ/WRITE access to OTHER files
- Exit MANAGE MODE by typing ***exit*** <RET>.

3. Using the TFTP client on the remote workstation, TFTP the `UPGRADE.OSW` file to the CyberSWITCH in binary mode. Be sure to include the file's full pathname. The exact method to transfer varies, depending upon your TFTP client.

   Note: If you experience a transmission timeout, check the retransmission setting on the TFTP package. A retransmission rate of 10 seconds is usually sufficient; values less than that may not work properly.
   If you experience a problem transferring the file with TFTP, wait about three minutes for the TFTP to fail, delete the incomplete file, and try again.

4. Using Telnet, reboot the system by issuing the command:
   restart

   It should take approximately 3 minutes for the system to restart and install the upgrade.

5. Login via Telnet and type the ***ver*** command to confirm that the system software upgraded correctly. If the upgrade did not occur, check the system log with the ***dr*** command to find any potential problems, and retry.

CHANGE DEFAULTS TO SECURE SYSTEM

The system is preconfigured with defaults that were designed to make it possible to have your system up and running quickly. After your machine is functioning properly, some of these defaults should be changed to make your system more secure. The following configuration changes are needed to provide this security:

1. Either delete User1 and User2 or change their names and secrets.

   Use Dynamic Management's manage mode to carry out either of these functions. To enter the manage mode, type ***manage*** at the system prompt. If you have no need for these types of devices (PPP devices), simply delete these two devices. At the manage mode prompt, enter the following command:
   device delete

   Follow the on-screen instructions for deleting each device.

   To change the preconfigured devices' names and secrets to secure the access to the system, enter the following command at the manage mode prompt:
   device change

   Follow the prompts to change the device name and secret for User1 and User2. After you have either deleted or changed the device information, make these changes permanent by entering the ***commit*** command

2. Disable TFTP Server.

   Disable through Dynamic Management's manage mode. This will secure important device information. Device information must be secure to prevent unauthorized access to the CyberSWITCH. To disable this access, enter the following command at the manage mode prompt:

   ```
   tftp change
   ```

   Then follow the on-screen instructions to disable the TFTP feature.

3. Change the admin and guest system passwords.

   If your system was previously accessed by your distributor, the preconfigured password will be *admin* (in lower case). Change this password to secure your system. To make this change, enter the following command at the system prompt:

   ```
   pswd
   ```

   Then follow the prompts to enter a new password. Your password must be a 3 to 16 nonblank character string. Be careful, passwords are uppercase and lowercase sensitive.

RETURN CONFIGURATION TO FACTORY DEFAULTS

The default configuration files are located on the *CSX150 Documentation and Set-Up Utility* CD. If you wish to return to the default configuration, download the `DEFLTCFG.OSW` file. Follow the same steps for Local or Remote Upgrade except you download the file `DEFLTCFG.OSW` instead of the `UPGRADE.OSW` file.

INITIAL INSTALLATION STEPS

There are initial configuration steps you must complete (regardless of remote device connections). We outline these steps in the following sections.

BEGINNING THE CONFIGURATION PROCESS

1. When you power on your system, the CyberSWITCH program automatically starts. Enter your log-in id (`admin`). Next, enter a password.

2. Start up the configuration editor, CFGEDIT; at the system prompt, type:

   ```
   cfgedit
   ```

   Note: If you are unsure of any configuration values, use the defaults.

   Use the displayed CFGEDIT menu to complete the remaining configuration steps.

PHYSICAL RESOURCE CONFIGURATION

1. Select *Physical Resources* from the main menu. Then, select *Resource* to display your CyberSWITCH's resources.

2. If you are not using the default switch type, press 1 to change the switch type.

3. Configure the WAN line. Select *Data Line* from the Physical Resources menu. After you select to add a line you will be prompted for the line name. Enter LINE1 for the first line name.

   For line information:
   - select point-to-point for the interface type
   - add a data link (two for DMS and NI-1 switch types)
   - use Automatic TEIs for these data links
   - select voice and data as your mode of operation (this will work for all connection types, including POTS connections)

   For async modem port information
   - if you are using the AMP port for a null modem, enter "NULLMODEM", if you are using the AMP port for a regular modem, enter a name you define for the modem
   - enter the baud rate
   - enter the data bits
   - enter the stop bits
   - enter the parity value
   - select the flow control type
   - select mode: either autosense or term

   If you are unsure of any of the above values, use the default value. If the default does not work, refer to your modem user documentation for their recommended values.

4. If you are using any accesses besides switched accesses (such as dedicated accesses, frame relay or X.25) configure the access now. Select *Access*. Select the type of access you wish to configure. Follow the on-screen instructions to complete the configuration.

   Note: Frame relay and X.25 accesses are available only if you have purchased the additional software module for packet switched accesses.

The initial configuration steps on the CyberSWITCH are now complete. Press <return> repeatedly until you return to the main CFGEDIT menu. Continue with the *Connectivity* section to complete remaining configuration steps.

CONNECTIVITY

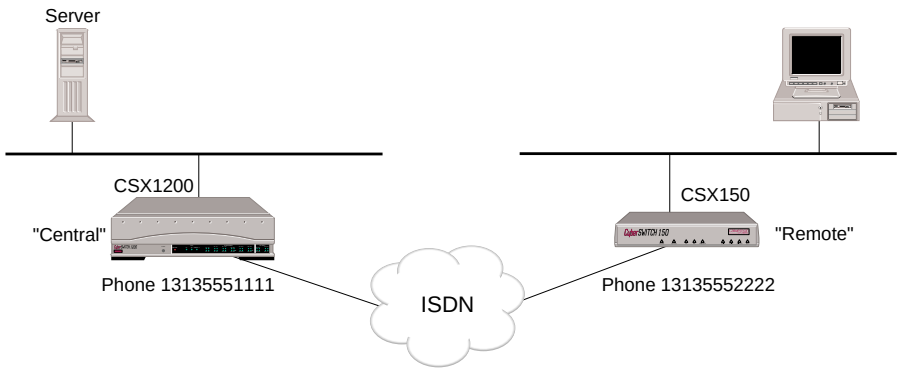
OVERVIEW

The Small Office CyberSWITCH can communicate with various other CyberSWITCH products via a PPP connection. This connection can be used to transmit data and provide remote management of your remote systems with Telnet, TFTP and SNMP. We will describe how to set up a PPP connection with other CyberSWITCH systems. For these examples, we are assuming that CyberSWITCH *"Remote"* is the remote system, and will want to call into CyberSWITCH *"Central"*; *Central* may or may not want to call *Remote*.

CONNECTING ONE CABLETRON PRODUCT TO ANOTHER VIA PPP

In this section, we describe the configuration steps required for connecting two of our products together via PPP. Separate instructions are included for bridging, IP routing with an UnNumbered Interface, IPX routing, and AppleTalk routing configurations.

BRIDGE TO BRIDGE CONFIGURATION



Configuration for Site "Central"

The configuration on *Central* to allow Bridging to *Remote* using PPP is as follows:

1. Perform initial configuration steps.
2. Select *Options* from the main menu.
3. Select *Bridging* from the options menu, then ensure that bridging is enabled.
4. Select *IP Routing* from the options menu, then disable IP routing to allow timely bridging of IP data.

5. Under Security, select *System Options and Information*, then under System Information:
   a. Set your System Name (*Central*). This matches up with *Central* device information configured on *Remote*.
   b. Set your System Secret (*Central_S*). This matches up with *Central* device information configured on *Remote*.

6. Under Security, select *Device Level Databases*, select *On-node Device Entries*, then add a device where the Device Name (*Remote*) must match the system name on *Remote*. When you add the device you must then enter the following information:
   a. Under ISDN Information select *ISDN Line Protocol*, then select *PPP*.
   b. Optional: If you wish to dial out to *Remote*, under ISDN Information, enter a dial out number (13135552222) and a base data rate (64Kb).
   c. Under Authentication you must:
      - Change CHAP Secret so that it matches *Remote's* System secret (*Remote_S*).
      - Optional: Configure Calling Line Ids (if Calling Line Id security was enabled).
   d. Under Bridge Information you must:
      - Make sure that Bridging is enabled
      - Optional: If you wish to dial out to *Remote* you must enable *Make calls for Bridge Data*.

5. Optional: If you wish to dial out to *Remote* you have to specify the method that you will use determine how to make bridge dial out calls. The two methods, and how to configure them are listed below:
   a. Select *Options* from the main menu, then the bridging menu, and from the bridging menu select bridge filters. Set up a Bridge filter with *connect* as the action. For some filter types you will need to specify *Remote* as the device.
   b. Select *Options* from the main menu, then the bridging menu, and from the bridging menu select Known Connect List, then enter the name of the Device (*Remote*) that you wish to call if a packet is received whose MAC address is known to be at the location that was connected earlier by the User's device.

   For a more detailed description of each of the above methods, refer to the *Installation Guide's* chapter titled *Configuring Advanced Bridging*.

CONFIGURATION FOR SITE "REMOTE"

The configuration on *Remote* so that it may use bridging to *Central* using PPP is as follows:

1. Perform initial configuration steps.

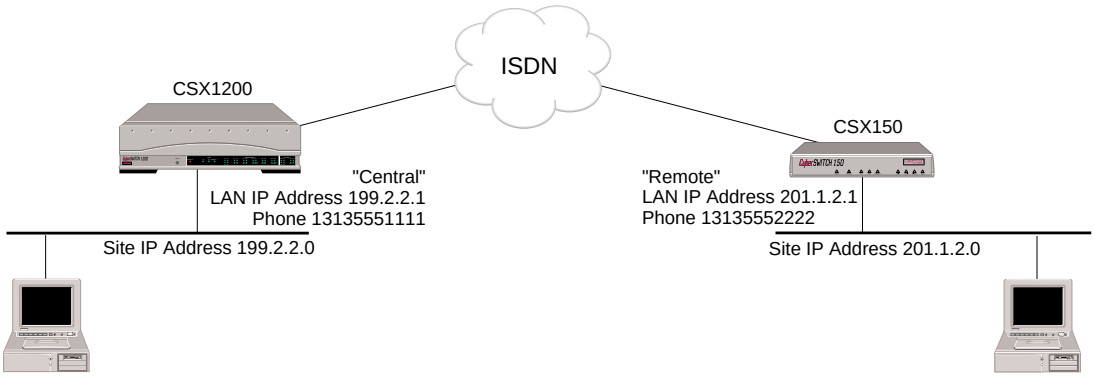
2. Under *Options*, select *Bridging* and make sure that it is enabled. Also, select *IP routing* and disable IP routing to allow timely bridging of IP data.

3. Under Security, select *System Options and Information*, then under System Information:
   a. Set your System Name (*Remote*). This matches up with *Remote* device information configured on *Central*.
   b. Set your System Secret (*Remote_S*). This matches up with *Remote* device information configured on *Central*.

4. Under Security, select *Device Level Databases*, select *On-node Device Entries*, then add a device where the Device Name (*Central*) must match the system name on *Central*. When you add the device you must then enter the following information:
   a. Under ISDN Information make sure the ISDN Line Protocol is PPP.
   b. Under ISDN Information you must enter a dial out number (13135551111) and a base data rate (64Kb).
   c. Under Authentication you must:
      - Change CHAP Secret so that it matches *Central's* System secret (*Central_S*).
      - Optional: Configure Calling Line Ids (if Calling Line Id security was enabled).
   d. Under Bridging you must:
      - Make sure that Bridging is enabled
      - Make sure that *Make calls for Bridge Data* is enabled.

5. Under Options, select *Bridging*, then select *Bridge Dial Out*. Make sure dial out is enabled. Then add the device (*Central*) that you wish to call when you receive a ethernet packet that is not on the same LAN as *Remote*. Note that the bridge dial out configuration is slightly different for *Remote* than it was for *Central*.

IP ROUTER TO IP ROUTER CONFIGURATION



CONFIGURATION FOR SITE "CENTRAL"

The configuration on *Central* to allow IP Routing to *Remote* using PPP is as follows:

1. Perform initial configuration steps.

2. Under Options, select *Bridging*, then disable Bridging. Select *IP Routing*, then:
   a. Enable IP Routing.
   b. Under IP Interfaces add a LAN Interface (IP address 199.2.2.1).
   c. Under IP Interfaces add a WAN UnNumbered Interface.

3. Under Security, select *System Options and Information*, then under System Information:
   a. Set your System Name (*Central*). This matches up with *Central* device information configured on *Remote*.
   b. Set your System Secret (*Central_S*). This matches up with *Central* device information configured on *Remote*.

4. Under Security, select *Device Level Databases*, select *On-node Device Entries*, then add a device where the Device Name (*Remote*) must match the system name on *Remote*. When you add the device you must then enter the following information:
   a. Under ISDN Information select *ISDN Line Protocol*, then select *PPP*.
   b. Optional: If you wish to dial out to *Remote*, under ISDN Information you must enter a dial out number (13135552222) and a base data rate (64Kb).
   c. Under Authentication you must:
      - Change CHAP Secret so that it matches *Remote's* System secret (*Remote_S*).
      - Optional: Configure Calling Line Ids (if Calling Line Id security was enabled).
   d. Under IP Information you must configure an IP Address of 0.0.0.0 for *Remote* since this is an unnumbered network interface. You should also check to make sure that IP Routing is on and Callable by IP is on.

5. Return to the Options menu, select *IP Routing*, then select *Static Route*. You will have to configure a static route to the 201.1.2.0 LAN. When you configure a static route to a site that uses a unnumbered interface you must enter the device name of the next hop device, *Remote* in this case.

CONFIGURATION FOR SITE "REMOTE"

The configuration on *Remote* to allow IP Routing to *Central* using PPP is as follows:

1. Perform initial configuration steps.

2. Under Options, select *Bridging*, then disable bridging. Select *IP Routing*, then:
   a. Enable IP Routing.
   b. Under IP Interfaces change the LAN Interface IP address (201.1.2.1).
   c. Under IP Interfaces make sure you have a WAN UnNumbered Interface.

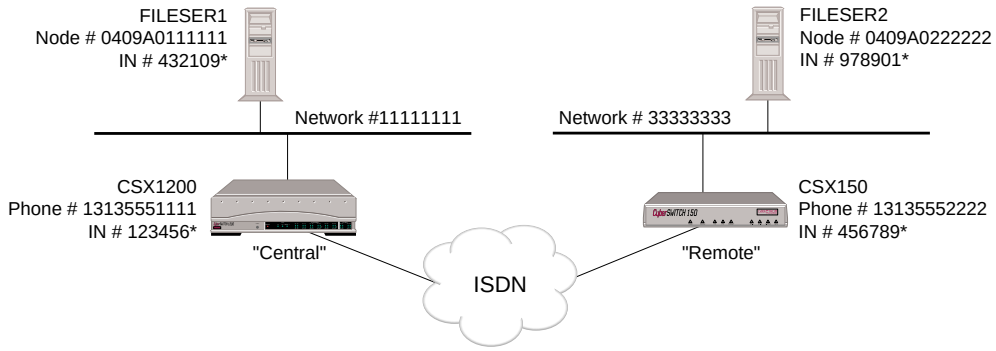
3. Under Security, select *System Options and Information*, then under System Information:
   a. Set your System Name (*Remote*). This matches up with *Remote* device information configured on *Central*.
   b. Set your System Secret (*Remote_S*). This matches up with *Remote* device information configured on *Central*.

4. Under Security, select *Device Level Databases*, select *On-node Device Entries*, then add a device where the Device Name (*Central*) must match the system name on *Central*. When you add the device you must then enter the following information:
   a. Under ISDN Information select *ISDN Line Protocol* then select *PPP*.
   b. To dial out to *Central*, under ISDN Information you must enter a dial out number (13135551111) and a base data rate (64Kb).
   c. Under Authentication you must:
      - Change CHAP Secret so that it matches *Central's* System secret (*Central_S*).
      - Optional: Configure Calling Line Ids (if Calling Line Id security was enabled).
   d. Under IP Information you must configure an IP Address of 0.0.0.0 for *Central* since this is an unnumbered network interface. You should also check to make sure that IP Routing is on and Callable by IP is on.

5. Return to the Options menu, select *IP Routing*, then select *Static Route*. You will have to configure a static route to the 199.2.2.0 LAN. When you configure a static route to a site that uses a unnumbered interface you must enter the device name of the next hop device, *Central* in this case.

IPX ROUTER TO IPX ROUTER CONFIGURATION

Note: This configuration illustrates IPXWAN routing only. If you are interested in configuring a remote LAN interface (to connect a CyberSWITCH to remote bridge devices), refer to the *Example Networks* Guide.



* IN # = Internal Network Number

CONFIGURATION FOR SITE "CENTRAL"

The configuration on *Central* to allow IPX Routing to *Remote* using PPP is as follows:

1. Perform initial configuration steps.

2. Under Options, select *IPX Routing*, then:
   a. Enable IPX Routing.
   b. Under IPX Internal Network Number enter the following value: *123456*.
   c. Under IPX Interfaces add a LAN Interface and a hexadecimal IPX Network Number (11111111).

3. Under Security, select *System Options and Information*, then under System Information:
   a. Set your System Name (*Central*). This matches up with *Central* device information configured on *Remote*.
   b. Set your System Secret (*Central_S*). This matches up with *Central* device information configured on *Remote*.

4. Under Security, select *Device Level Databases*, select *On-node Device Entries*, then add a device where the Device Name (*Remote*) must match the system name on *Remote*. When you add the device you must then enter the following information:
   a. Under ISDN Information select *ISDN Line Protocol*, then select *PPP*.
   b. Optional: If you wish to dial out to *Remote*, under ISDN Information you must enter a dial out number (13135552222) and a base data rate (64Kb).

c. Under *Authentication* you must:
   - Change CHAP Secret so that it matches *Remote's* System secret (*Remote_S*).
   - Optional: Configure Calling Line Ids (if Calling Line Id security was enabled).

d. Under *IPX Information*:
   - enable *IPX*
   - enable *Make Calls for IPX data*
   - enable *IPXWAN protocol*
   - select *Triggered RIP/SAP* with a WAN peer type of *ACTIVE* from the *Routing Protocol* option

Note: By using triggered RIP/SAP, you do not need to configure static routes or services.

CONFIGURATION FOR SITE "REMOTE"

The configuration on *Remote* to allow IPX Routing to *Central* using PPP is as follows:

1. Perform initial configuration steps.

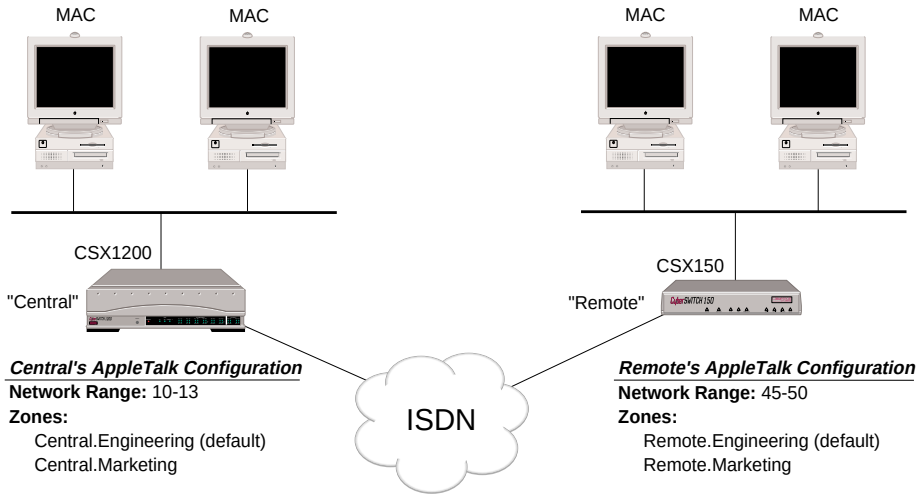
2. Under Options, select *IPX Routing*, then:
   a. Enable IPX Routing.
   b. Under IPX Internal Network Number enter the following value: *456789*.
   c. Under IPX Interfaces add a LAN Interface and a hexadecimal IPX Network Number (33333333).

3. Under Security, select *System Options and Information*, then under System Information:
   a. Set your System Name (*Remote*). This matches up with *Remote* device information configured on *Central*.
   b. Set your System Secret (*Remote_S*). This matches up with *Remote* device information configured on *Central*.

4. Under Security, select *Device Level Databases*, select *On-node Device Entries*, then add a device where the Device Name (*Central*) must match the system name on *Central*. When you add the device you must then enter the following information:
   a. Under ISDN Information select *ISDN Line Protocol* then select *PPP*.
   b. Under ISDN Information you must enter a dial out number (13135551111) and a base data rate (64Kb) to dial out to *Central*.
   c. Under Authentication you must:
      - Change CHAP Secret so that it matches *Central's* System secret (*Central_S*).
      - Optional: Configure Calling Line Ids (if Calling Line Id security was enabled).
   d. Under *IPX Information*:
      - enable *IPX*
      - enable *Make Calls for IPX data*
      - enable *IPXWAN protocol*
      - select *Triggered RIP/SAP* with a WAN peer type of *ACTIVE* from the *Routing Protocol* option.

Note: By using triggered RIP/SAP, you do not need to configure static routes or services.

APPLETALK ROUTER TO APPLETALK ROUTER CONFIGURATION



CONFIGURATION FOR SITE "CENTRAL"

The configuration on *Central* to allow AppleTalk Routing to *Remote* is as follows:

1. Perform initial configuration steps.

2. Under Security, select *Device Level Databases*, select *On-node Device Entries*, then add a device where the Device Name (*Remote*) must match the system name on *Remote*. When you add the device you must then enter the following information:
   a. Under ISDN Information select *ISDN Line Protocol*, then select *PPP*.
   b. Optional: If you wish to dial out to *Remote*, under ISDN Information you must enter a dial out number and a base data rate (64Kb).
   c. Under Authentication you must:
      - Change CHAP Secret so that it matches *Remote's* System secret (*Remote_S*).
      - Optional: Configure Calling Line Ids (if Calling Line Id security was enabled).
   d. Under AppleTalk Information you must:
      - Enter 0.0 for the AppleTalk address.
      - Enable AppleTalk Routing.
      - Enable making calls for AppleTalk data.

3. Under Options, select *AppleTalk Routing*, then:
   a. Enable AppleTalk routing.
   b. Under AppleTalk Port Information, configure a LAN port:
      - Select the *LAN* port type.
      - Enter *lanport1* for the port name.
      - Enter *1* for the LAN port number.
      - Select the *Extended* network type (the default).
      - Enter *10-13* for the network range.
      - Accept the default of *none* for the suggested AppleTalk address.
      - Enter *Engineering* as the port's default zone name.
      - Enter *Marketing* as the second zone name.

c. Under AppleTalk Port Information, configure a WAN UnNumbered port:
   - Select the WAN UnNumbered port type.

d. Under AppleTalk Static Routes, configure a static route to *Remote*:
   - Enter *Extended* for *Remote's* network type (the default).
   - Enter *45-50* as the destination network range (*Remote's* network range).
   - Enter *0.0* as the next hop (it's over an unnumbered link).
   - Enter *Remote* as the next hop's device name.
   - Enter *2* as the number of hops for this route.
   - Enter *Remote.Engineering* as *Remote's* default zone name.
   - Enter *Remote.Marketing* as *Remote's* second zone name.

4. Under Security, select *System Options and Information*, then under System Information:
   a. Set your System Name (*Central*). This matches up with *Central* device information configured on *Remote*.
   b. Set your System Secret (*Central_S*). This matches up with *Central* device information configured on *Remote*.

CONFIGURATION FOR SITE "REMOTE"

The configuration on *Remote* to allow AppleTalk Routing to *Central* is as follows:

1. Perform initial configuration steps.

2. Under Security, select *Device Level Databases*, select *On-node Device Entries*, then add a device where the Device Name (*Central*) must match the system name on *Central*. When you add the device you must then enter the following information:
   a. Under ISDN Information select *ISDN Line Protocol*, then select *PPP*.
   b. Optional: If you wish to dial out to *Central*, under ISDN Information you must enter a dial out number and a base data rate (64Kb).
   c. Under Authentication you must:
      - Change CHAP Secret so that it matches *Central's* System secret (*Central_S*).
      - Optional: Configure Calling Line Ids (if Calling Line Id security was enabled).
   d. Under AppleTalk Information you must:
      - Enter 0.0 for the AppleTalk address.
      - Enable AppleTalk Routing.
      - Enable making calls for AppleTalk data.

3. Under Options, select *AppleTalk Routing*, then:
   a. Enable AppleTalk routing.
   b. Under AppleTalk Port Information, configure a LAN port:
      - Select the *LAN* port type.
      - Enter *lanport1* for the port name.
      - Enter *1* for the LAN port number.
      - Select the *Extended* network type (the default).
      - Enter *45-50* for the network range.
      - Accept the default of *none* for the suggested AppleTalk address.
      - Enter *Remote.Engineering* as the port's default zone name.
      - Enter *Remote.Marketing* as the second zone name.

c. Under AppleTalk Port Information, configure a WAN UnNumbered port:
   - Select the WAN UnNumbered port type.

d. Under AppleTalk Static Routes, configure a static route to *Central*:
   - Enter *Extended* for *Central's* network type (the default).
   - Enter *10-13* as the destination network range (*Central's* network range).
   - Enter *0.0* as the next hop (it's over an unnumbered link).
   - Enter *Central* as the next hop's device name.
   - Enter *2* as the number of hops for this route.
   - Enter *Engineering* as *Central's* default zone name.
   - Enter *Marketing* as *Central's* second zone name.

4. Under Security, select *System Options and Information*, then under System Information:
   a. Set your System Name (*Remote*). This matches up with *Remote* device information configured on *Central*.
   b. Set your System Secret (*Remote_S*). This matches up with *Remote* device information configured on *Central*.

SPECIAL FEATURES

CONFIGURING THE POTS OPTION

The dual-line, Plain Old Telephone Service (POTS) feature allows one or both of the ISDN B-channels to alternatively be used with traditional phone equipment, including faxes and answering machines. The CyberSWITCH can use both B-channels for data until a call is initiated or received. When a call comes up, the CyberSWITCH may then drop back to a single B-channel for data, and reserve the other B-channel for POTS use (such as voice or fax).

The POTS service supports 3.1 Khz Audio or Speech service. This service guarantees the proper channel bandwidth in regard to the phone companies.

Each of the two POTS ports may have either the same or different phone numbers. If each port has its own number, each has its own data link allocated to it.

POTS supports the *alternate outbound* and *forward incoming* call features. These features, if enabled, recognize when a second data link is available, and automatically uses it when its allocated data link is busy. For example, in a one-person sales office, you could use the *forward incoming* feature to always ring on the first line, which would attach to the telephone on your desk. However, if your line were busy, the call would automatically be routed to the second line, which is attached to an answering machine.

To use the POTS interface, configure the following:

- POTS devices
- the CyberSWITCH POTS information including:
  the encoding standard
  the POTS lines configuration information
- per user POTS priority information

Refer to the next section for a description of configuring CyberSWITCH POTS information.

CONFIGURING THE ENCODING STANDARD

The encoding standard is the type of standard for tone feeding and ring feed. This should be set properly on the switchtype. Only change the value of the encoding standard if you are having difficulties. To select the encoding standard:

1. Select *Physical Resources* from the main CFGEDIT menu.

2. Select *POTS* from the Physical Resource Menu.

3. Select *Encoding Standard* from POTS Menu.

4. Enter the Id of the encoding standard you wish to use (from displayed list).

CONFIGURING POTS LINE INFORMATION

To use the POTS feature, you must configure a POTS line. POTS line information includes: the POTS line jack Id, the primary phone number (optional), and customization information (also optional).

The section below describes configuring the POTS line information.

1. Select *Physical Resources* from the main CFGEDIT menu.
2. Select *POTS* from the Physical Resource Menu.
3. Select *Lines* from the POTS Menu.
4. *Press 1* to add a POTS line.
5. Select the jack Id from the list of available jacks.
6. Optional: enter the primary phone number of the POTS line.
   Select your primary phone number from the displayed list. This list is the directory numbers you configured for your data links. There will be no list displayed if there are no data links configured.
7. Optional: customize POTS configuration.
   a. Enable or disable *Use Alternate Outbound if Primary is Busy*.
      If you enable this option, an outbound call from the specified jack can use any available datalink (that supports *voice* or *voice+data*) if the primary phone number is busy. This option is necessary for applications using Calling Line Id for the POTS jacks. If you disable this option, outbound calls will only use the configured datalink and phone number.
   b. Enable or disable *Forwarding Incoming if Other Jack is Busy*.
      If you enable this option, incoming calls to a particular jack can be sent to the other jack if the first jack is busy. If you disable this option, the CyberSWITCH will reject the incoming call.
   c. Select the *Type of Device Connected to this Jack*. Select *telephone* or *other*.

CONFIGURING POTS INFORMATION PER DEVICE

To configure the POTS information per device:

1. Select *Security* from the main CFGEDIT menu.
2. Select *Device Level Databases* from the security menu.
3. Select *On-node Device Entries* from the authentication database menu.
4. Enter non-POTS device information.
5. To enter POTS information, select *POTS Priority Information*.

6. From the displayed list, select the type of POTS priority you want for this device.
   a. You may select *Preemption of 2nd B-Channel by POTS* when both B-channels are active to this device. If you select this priority, one of the two active data calls to this device will be preempted to service an incoming / outgoing phone call.
   b. You may select *Disconnection by POTS for Last B-Channel* when a single B-channel is used for a data call for this device. If you select this priority, this last B-channel may be disconnected to service an incoming / outgoing phone call. By configuring this option, you are implicitly enabling preemption of this device.
   c. You may also select *None of the above*. If you select this priority, the CyberSWITCH will not preempt or disconnect any active data calls to service an incoming / outgoing phone call.

CONFIGURING HARDWARE FILTERS

This feature allows the CyberSWITCH to increase its bridging performance when heavy local unicast traffic is present. Hardware filters let you move the burden of filtering the unicast local traffic from the CPU to the ethernet controller. This results in both an increase in performance and a reduction in dropped packets. As a default, this feature is disabled.

Note: If bridging is disabled, hardware filters have no affect.

In order to use hardware filters, the CyberSWITCH must have a list of destination MAC addresses. The CyberSWITCH obtains the addresses in two ways: manually and automatically.

In the *manual mode*, you enter the list of destination MAC addresses. When the CyberSWITCH software initializes in this mode, no bridge learning occurs. Instead, the bridge will skip the learning phase and move directly to the forwarding phase. The CyberSWITCH will check to see if the incoming packet's destination bridge address is on the configured list of addressees. Thus, when a packet destined for one of the addresses in the list is received, it will be bridged normally. Multicast frames are handled the same regardless of whether this feature is enabled or not. Unicast frames destined for MAC addresses not configured manually will not be bridged. Up to 63 destination MAC addresses can be configured in this mode.

In the *auto mode*, you specify a time limit for learning MAC addresses and the maximum number of addresses the CyberSWITCH can learn. When the CyberSWITCH software initializes in this mode, the bridge will use its normal phases. Once it reaches the forwarding phase, bridging will progress as if hardware filtering were not enabled. As the bridge learns about remote MAC addresses, they are added to the MAC address list for hardware filtering. Once either the time limit or the limit of number of addresses is reached, the hardware filtering feature will be enabled. A message is then written to the log.

To configure the hardware filters feature:

1. Select *Options* from the main CFGEDIT menu.

2. Select *Bridging* from the options menu.

3. If bridging is not enabled, follow the onscreen instructions to enable bridging.

4. Select *Enable/Disable the MAC H/W Filtering Feature* from the bridging menu.

5. Follow onscreen instructions to enable hardware filtering.

6. Select *Mode of H/W Filtering* from the bridging menu.

7. Select your mode of hardware filtering from the displayed list.

8. If you have selected *Manual Mode*:
   a. Select *Bridge Filters* from the bridging menu.
   b. Select *Hardware Filters* from the filters menu.
   c. Enter the MAC addresses you want to include.

9. If you have selected *Auto Mode*:
   a. Select *Bridge Filters* from the bridging menu.
   b. Select *Hardware Filters* from the filters menu.
   c. Select *Maximum Number of Addresses to Learn*, enter a value for the maximum.
      After the maximum number of addresses to learn has been met, the CyberSWITCH stops learning addresses and enters the forwarding state.
   d. Select *Address Learning Time-Out*, enter the time-out value.
      After the time-out value has been met, the CyberSWITCH stops learning MAC addresses, and enters the forwarding state.
   e. Select *Enable/Disable Flush & ReLearn Time-Out*, select either enable or disable.
      If you enable this feature, after the configured time-out value (see next item) all MAC addresses are erased, and the learning process begins again.
   f. Select *Flush &ReLearn Time-Out*, enter the time-out value.
      The time frame for flushing out all MAC addresses and starting the learning process over again.

TROUBLESHOOTING

The front panel of the CyberSWITCH has several LED indicators. Refer to page 20 for an illustration of the front panel. The *Power* indicator will remain lit while the unit is on. There is a series of three LAN indicators: they light up indicating transmissions, receptions, or good link integrity on the 10Base-T port. The WAN indicators include the *Sync*, *D-Chan*, *CH-1*, and *CH-2*. Detailed descriptions of the indicators follow.

LOCAL AREA NETWORK LED INDICATORS

There are three LAN indicators: *TX*, *RX*, and *10BaseT*. These three indicators provide information about the state of the communication link between the CyberSWITCH and the LAN to which it is connected.

1. The *10BaseT* indicator signifies connection to a 10Base-T LAN. If there is good link integrity on the 10Base-T port, this light shines steadily. If a connection other than 10Base-T is used (such as an AUI connection) or there is no link integrity, this light will not shine.

2. The *TX* indicator signifies that the CyberSWITCH has transmitted data to the LAN. *TX* flashes whenever the CyberSWITCH sends at least 128 bytes of data on the LAN.

3. The *RX* indicator signifies that the CyberSWITCH is receiving data from another device on the LAN to which it's connected.

WIDE AREA NETWORK LED INDICATORS

The bank of four LED indicators make up the Wide Area Network (WAN) LED indicators. The WAN LED indicators provide information on the status of the BRI line. The four LED indicators include: *Sync*, *D-Chan*, *CH-1*, and *CH-2*.

- The *Sync* indicator identifies whether or not the most basic level of the ISDN connection (Layer 1) is established. It verifies that the CyberSWITCH is connected to the ISDN network at this BRI port. This light must be on for D-CHAN, CH-1 or CH-2 to be operational.

- The *D-Chan* indicator signifies data link and D-channel activity. If the D channel is active, the indicator flashes. When a call goes up, the *D-Chan* indicator flickers momentarily, and then turn on as the *CH-2* indicator turns on. With a second call, the *D-Chan* indicator flickers momentarily and then the *CH-1* indicator turns on.

D-CHAN LED status	*One Data Link*	*Multiple Data Links**
off	no activity	no activity
flashing (mostly off)	trying to bring up data link	not all data links are up
flashing (mostly on)	activity data link is up	activity data link is up
on solid	no activity data link is up	no activity data link is up

* On DMS-100 and NI-1 switches, more than one data link is possible.

- The *CH-1* and *CH-2* indicators signify activity along their respective B channel:

CH-1 or CH-2 LED Status	*Description*
off	no call over channel
flashing	Data being passed over channel. Speed of flashes depends upon number of frames being sent.
on solid	call up, but no data being transferred

SERVICE INDICATOR

The *Service* indicator is the only indicator that is red. It comes on normally during system power-up, and then goes off. If the *Service* indicator remains lit or blinks after power-up, it is signaling that something needs attention in the system. If this occurs, access your administrative console for further information.

SERVICE INDICATOR REMAINS LIT

If the *Service* indicator remains lit during the power-on sequence, this means the CyberSWITCH software is unable to boot. The CyberSWITCH may be having some type of operational problem. While the *Service* indicator remains lit, the other LEDs will blink a certain number of times, pause, then blink that number of times again (See following table). This pattern will be repeated five times. The actions to take if this occurs are:

1. Make note of the number of consecutive blinks.

2. Restart the CyberSWITCH.

3. If the *Service* LED is still lit, and the other LEDs are still flashing, contact your distributor and provide them with the count of consecutive blinks.

The table below provides an error description corresponding to the number of consecutive LED blinks:

Number of Blinks	*Error Description*
1	Failure during erasure of main block during SSB* recovery
2	Failure during programming of main block during SSB recovery
3	Timed out during recovery of SSB
4	Individual record error during recovery of SSB
5	Communications error during recovery of SSB
6	Incompatibility between FSB* and new SSB versions
7	Currently not used
8	Bad address information contained in SSB received during recovery
9	SSB, received during Recovery, contained a bad checksum for entire image

* FSB: First Stage Boot; SSB: Second Stage Boot.

SERVICE INDICATOR BLINKS

If the *Service* indicator blinks at any time during CyberSWITCH operation, access your administrative console (using the *status* command) for further information. One or more of the following messages should be displayed:

- OUT SVC 1
- OUT SVC 2
- OUT SVC 3
- OUT SVC 4
- OUT SVC 5
- LAN XMIT ERROR

These messages indicate a problem with the LAN or BRI connections, or an incorrectly programmed SPID.

The *Service* indicator will also blink if semipermanent devices are configured, and a connection to one of these devices is faulty. Use the *sp* command to check the status of the semipermanent connection. Once you correct the problem, the *Service* indicator will automatically turn off.

INDEX

Numerics

10Base2 (BNC) cabling 12
10BaseT
- direct cabling 10
- hub cabling 9
- indicator 45
- LED indicator 20

A

address learning time-out 44
alternate outbound 41
alternate outbound (POTS) 42
AMP connections 13
auto mode (hardware filters) 43
automatic TEIs 31

B

battery replacement 21
BNC cabling 12

C

cabling 8
- AMP connections 13
- ISDN connections 15
- Nomad to PC connections 8
- POTS connection 18
- power connections 19

CFGEDIT 24
cfgedit 30
compliance notices 3
configuration tools 23

D

data links 31
D-CHAN indicator 20, 45
defaults
- returning to factory defaults 30
- system defaults 29

DOC notice 4
DSU 17

E

encoding standard (POTS) 41
exit 24

F

factory defaults 30
FCC notice 3
flush & relearn 44
forward incoming (POTS) 41, 42

H

hardware filters 43
- auto mode 43
- configuring 43
- manual mode 43

I

ISDN connections 15

L

LAN connections
- 10Base2 12
- 10BaseT direct 10
- 10BaseT Hub 9

LAN indicators 45
LED indicators 20, 45
- 10BaseT 20
- D-CHAN 20
- LAN 45
- power indicator 20
- RX indicator 20
- service 46
- SYNC 20
- WAN 45

logging in 23
log-in id 30

M

manage 24
Manage Mode 24
manual mode (hardware filters) 43
messages
- LED indicators 45

N

NT-1 15, 16

P
POTS 41
call features 41
configuration 41
configuration requirements 41
connection 18
line information 42
phone numbers 41
speech service 41
user information 42
power connection 19
power indicator 20

R
real-time management mechanism
dynamic management feature 24
remote devices 45
via PPP 32
restart 22
RX indicator 20, 45

S
S/T interface
and the termination switches 17
safety considerations 21
security
securing the system 29
service indicator 20, 46
Setup Utility 23
SYNC indicator 45
system defaults
changing to secure system 29

T
termination switches 17
tools for configuration 23
troubleshooting
using LED indicators 45
TX indicator 45

U
U interface
and the termination switches 17

V
VCCI notice 4

W
WAN LED indicators 45